

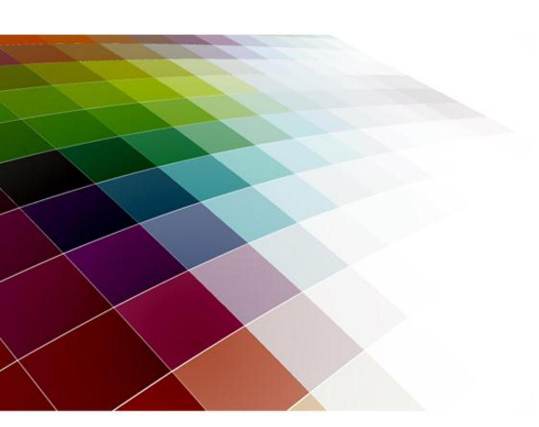
Rendez-vous annuel *[incontournable]*
du Comité Social Paris Ile-de-France











« L'utilisation des NTIC par le salarié :
limites et contrôle par l'employeur »





Partenaire Média







Maître Laurent Beljean,
Fromont Briens • Avocats spécialisés en droit social

« **L'utilisation des NTIC par le salarié :** limites et contrôle par l'employeur »







Sommaire

- Introduction
- Principes régissant l'utilisation des NTIC en droit du travail
- Les relations individuelles et les NTIC
- Les relations collectives et les NTIC





Introduction

Quelques définitions…

– Nouvelles Technologies de l'Information et de la Communication:

Elles regroupent les techniques utilisées dans le traitement et la transmission, des informations, principalement de l'informatique, de l'internet et des télécommunications.

– Données personnelles: article 2 de la loi du 6 janvier 1978, n°7817

« Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ».

– Traitement de données à caractère personnel: article 2 de la loi du 6 janvier 1978

« Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».





Partenaire Média



1. Principes régissant l'utilisation des NTIC en droit du travail

- 1.1. Obligations de l'employeur liées à l'utilisation des NTIC au sein de l'entreprise
- 1.2. Droits des salariés lors de l'utilisation des NTIC au sein de l'entreprise





1.1 Obligations de l'employeur liées à l'utilisation des NTIC au sein de l'entreprise

- 1.1.1. Procédure préalable à la mise en place d'un système de contrôle des salariés dans les locaux de travail
- 1.1.2 L'obligation de loyauté et de transparence
- 1.1.3 L'obligation de proportionnalité et de finalité
- 1.1.4 La collecte des données
- 1.1.5 La conservation des données personnelles
- 1.1.6 L'obligation de sécurité
- 1.1.7 L'obligation de confidentialité
- 1.1.8 L'obligation de déclaration





Partenaire Média



1.1.1 Procédure préalable à la mise en place d'un système de contrôle des salariés

- Article L 2323-32 du code du travail: information et consultation du comité d'entreprise. L'employeur doit présenter au CE un document d'information portant a minima sur:
  - La justification de la mise en place du dispositif de sécurité
  - Descriptif du système de surveillance
  - Modalités et durées de conservation des enregistrements
  - Procédure d'information des salariés
  - Procédure de déclaration à la CNIL

- Sanctions du défaut de consultation du CE:
  - Moyen de preuve illicite ou irrecevable
  - Délit d'entrave





Partenaire Média



1.1.1 Procédure préalable à la mise en place d'un système de contrôle des salariés

- Article L 4612-8: consultation du CHSCT
  - Consultation avant toute décision d'aménagement emportant modification des conditions de travail des salariés

- Information individuelle et préalable des salariés: article L1222-4 du code du travail dispose que « *Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance* »

- Moyens:
  - Information individuelle de tous les salariés
  - Affichage d'une note dans les locaux de travail





Partenaire Média



1.1.1 Procédure préalable à la mise en place d'un système de contrôle des salariés

- Déclaration à la CNIL
  - Loi du 6 janvier 1978, n°78-17 relative à l'informatique, aux fichiers et aux libertés impose à l'employeur de déclarer préalablement à la CNIL, la mise en place d'un système de « *traitement automatisé d'informations nominatives* »
  - Tout enregistrement et stockage d'images constituent une collecte de données nominatives dès lors qu'elle permet l'identification des salariés (8ème rapport de la CNIL)
  - Obligation de remplir le formulaire CERFA n°99001 lors de la mise en place d'un système de vidéosurveillance des salariés dans les locaux de travail

- Sanction du défaut de déclaration à la CNIL: article 226-16 du code pénal
  - Peine d'emprisonnement de 5 ans
  - Amende de 300 000 euros





Partenaire Média



1.1.1 Procédure préalable à la mise en place d'un système de contrôle des salariés

- Modification du règlement intérieur de l'entreprise
  - Conformément à l'article L 1321-1 du code du travail, le règlement intérieur s'impose aux salariés et permet notamment à l'employeur de fixer, unilatéralement, les mesures d'application de la réglementation en matière d'hygiène et de sécurité dans l'entreprise
  - A titre de rappel, la modification du règlement intérieur doit s'effectuer selon les règles prescrites par l'article L 1321-4 du code du travail:
    - Avis du comité d'entreprise et du CHSCT
    - Communication en deux exemplaires du règlement modifié et l'avis des représentants du personnel à l'inspecteur du travail
    - Dépôt du règlement intérieur au secrétariat greffe du CPH
    - Affichage sur les lieux du travail du règlement modifié





Partenaire Média



1.1.2 L'obligation de loyauté et de transparence

- Article 6 de la loi n°78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée par la loi n°2004-801 du 6 août 2004
- Les données doivent être collectées et traitées de manière loyale et licite par l'employeur
- Information obligatoire du salarié sur tout dispositif d'information le concernant
- Consultation du comité d'entreprise sur tous moyens et techniques permettant un contrôle de l'activité des salariés
- En application de ce principe, l'employeur doit, conformément aux dispositions de l'article 32 de la loi de 1978 modifiée, informer les salariés de :
  - La nature des informations transmises
  - La finalité du traitement des données
  - Des personnes physiques ou morales destinataires des données
  - Du droit d'accès et de rectification dont ils disposent





Partenaire Média



1.1.3 L'obligation de proportionnalité et de finalité

– Cette obligation résulte notamment de:

- L'article 6 de la loi n°78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée par la loi du n°2004-801 du 6 août 2004

- L'article 2 de la DDHC de 1789 : respect du droit à la vie privée

- L'article 9 du code civil relatif au droit de chacun au respect de sa vie privée

- L'article L 1121-1 du code du travail qui dispose : « *Nul ne peut porter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* »





1.1.3 L'obligation de proportionnalité et de finalité

- En conséquence:
  - Les données doivent être collectées pour des finalités:
    - Déterminées et explicites
    - Pertinentes et adéquates
    - Les informations demandées doivent être proportionnées au but recherché
  - Les données ainsi collectées doivent être justifiées par un intérêt légitime (exigence de sécurité, nécessité d'éviter un usage abusif de l'informatique à des fins personnelles, risque particulier de vols, surveillance d'un poste de travail dangereux, etc.) et ne pas être excessives au regard de ses finalités
  - Les données ne doivent pas être utilisées ultérieurement de manière incompatible avec la finalité pour laquelle elles ont été collectées
  - Si modification ou extension de la finalité, une déclaration complémentaire sera nécessaire



Partenaire Média



1.1.3 L'obligation de proportionnalité et de finalité

– Sanctions du détournement de la finalité des données recueillies: article 226-21 du code pénal:

- 5 ans d'emprisonnement
- 300 000 euros d'amende, voire 1 500 000 euros si le contrevenant est une personne morale





1.1.4 La collecte des données

- L'article L 1222-2 du code du travail dispose que: « *Les informations demandées, sous quelque forme que ce soit, à un salarié ne peuvent avoir pour finalité que d'apprécier ses aptitudes professionnelles. Ces informations doivent présenter un lien direct et nécessaire avec l'évaluation de ses aptitudes. Le salarié est tenu de répondre de bonne foi à ces demandes d'informations ».*

- En conséquence:
  - Par principe, il convient de recueillir le consentement du salarié pour utiliser une information collectée
  - Les données traitées doivent être exactes, complètes et si nécessaire, mises à jour
  - Il est interdit de mettre en mémoire ou conserver des données relatives aux origines raciales, opinions politiques, philosophiques ou religieuses, aux appartenances syndicales, à la santé, à la vie sexuelle, ou encore les infractions et condamnations encourues, à défaut peines encourues: 5 ans d'emprisonnement et 300 000 euros d'amende (article 226-19 du code pénal)





Partenaire Média



1.1.4 La collecte des données

- Au regard de l'article 6 de la loi du 6 janvier 1978
  - La collecte des données doit être légale et licite
  - Les finalités de cette collecte doit être déterminées, explicites et légitimes
  - Les données doivent être adéquates, pertinentes, non excessives au regard de leur finalité
  - Les données doivent être exactes, complètes et mises à jour

- Sanction d'une collecte de données personnelles par des moyens frauduleux, déloyaux ou illicites : article 226-18 du code pénal
  - 5 ans d'emprisonnement
  - 300 000 euros d'amende





Partenaire Média



1.1.5 La conservation des données personnelles

– L'article 6 de la loi du 6 janvier 1978 modifiée prévoit que les données à caractère personnel ne doivent pas être conservées pendant une durée qui excède la durée nécessaire eu égard aux finalités pour lesquelles elles sont collectées et traitées, sauf autorisation de la CNIL (CE, 18 mars 2005, n°238206)

– Cette durée s'apprécie donc selon la nature de la donnée

– Le non respect de cette formalité est sanctionné à l'article 226-20 du code pénal
  - 5 ans d'emprisonnement
  - 300 000 euros d'amende





Partenaire Média



1.1.5 La conservation des données personnelles

– A titre d'exemples, la CNIL recommande de conserver:
  - Données relatives à la paie: 5 ans
  - Fichiers de recrutement: 2 ans après le dernier contact client
  - Enregistrement des vidéosurveillances: 1 mois
  - Informations relatives aux absences des salariés: pas au-delà du temps nécessaire à l'établissement des fiches de paie
  - Informations nécessaires à l'établissement des droits du personnel, tel la retraite : sans limitation de durée





Partenaire Média



1.1.6 L'obligation de sécurité

- L'article 34 de la loi du 6 janvier 1978 modifiée impose à la personne qui ordonne ou effectue le traitement automatisé des données à caractère professionnel de prendre toutes les précautions utiles aux fins de préserver la sécurité des informations et notamment éviter qu'elles soient:
  - Déformées
  - Endommagées
  - Communiquées à des tiers non autorisés
- Sécurité assurée au moyens de logiciels de protection des données, de mots de passe, etc.
- Recommandation de la CNIL du 21 juillet 1981, n°81-094: les utilisateurs ou détenteurs de ces fichiers sont responsables du choix des mesures de sécurité
- Inexécution de cette obligation de sécurité sanctionnée à l'article 226-16 du code pénal
  - 5 ans d'emprisonnement
  - 300 000 euros d'amende, voire 1 500 000 euros si le responsable est une personne morale
  - Publication de tout ou partie du jugement





Partenaire Média



1.1.7 L'obligation de confidentialité

- Cette obligation résulte de:
  - L'article 34 de la loi du 6 janvier 1978 modifiée
  - L'article L 1222-3 du code du travail en matière d'évaluation professionnelle des salariés
  - L'article L 1221-8 du code du travail en matière de recrutement des salariés

- Principe: seules les personnes autorisées peuvent accéder aux données personnelles contenues dans les fichiers (salarié, inspection du travail, administration fiscale, etc.)

- Sanctions prévues à l'articles 226-22 du code pénal:
  - Divulgation à des tiers non autorisées des informations confidentielles est punie de 5 ans d'emprisonnement et 300 000 euros d'amende
  - Divulgation par imprudence ou négligence est punie de 3 ans d'emprisonnement et de 100 000 euros d'amende





Partenaire Média



1.1.8 L'obligation de déclaration

- Principe: le responsable du traitement automatisé ou non de données à caractère personnel doit effectuer une déclaration à la CNIL

- 3 hypothèses:
  - Déclaration ordinaire: pour les traitements à caractère personnel qui peuvent porter atteinte à la vie privée
  - Déclaration simplifiée: pour les catégories les plus courantes des traitements qui ne portent pas atteinte à la vie privée (article 24 loi 1978 modifiée), tels la gestion du personnel, la gestion des contrôle d'accès aux locaux de travail, des horaires et de la restauration, l'utilisation de services de téléphonie fixe ou mobile et la géolocalisation
  - Exonération de déclaration:
    - Fichiers de paie (délibération CNIL n°2004-097 du 9 décembre 2004)
    - Gestion des activités sociales et culturelles des comités d'entreprises ou d'établissements (délibération CNIL n°2006-230 du 17 octobre 2006)
    - Un correspondant à la protection des données a été désigné au sein de l'entreprise





Partenaire Média



1.1.8 L'obligation de déclaration

- **La déclaration ordinaire**: article 22 et 23 de la loi du 6 janvier 1978 modifiée
  - Cette déclaration doit être effectuée préalablement à la mise en œuvre du traitement
  - La société s'engage à ce que le traitement soit conforme aux exigences de la loi
  - Cette déclaration peut être adressée à la CNIL par voie électronique, par LR-AR ou dépôt au secrétariat de la CNIL, contre reçu
  - Mise en œuvre du traitement suite à la réception du récépissé de la déclaration de la CNIL

- **La déclaration simplifiée** doit comporter les mentions suivantes:
  - Les finalités des traitements faisant l'objet de la déclaration
  - Les données à caractère personnel
  - La ou les catégories de personnes concernées
  - Les destinataires auxquels les données sont communiquées
  - La durée de conservation





Partenaire Média



1.1.8 L'obligation de déclaration

- **Le correspondant à la protection des données** : Décret n°2005-1309 du 20 octobre 2005 modifié par le Décret n°2007-451 du 25 mars 2007
  - Sa désignation exonère l'employeur de son obligation de déclaration lors de la mise en place d'un traitement automatisé des données concernant son personnel
  - Missions:
    - Chargé de veiller, de manière indépendante, à la conformité des traitements à la législation et d'établir une liste de ces traitements accessible à toutes personnes en faisant la demande
    - Possibilité de faire toute recommandation au responsable des traitements
    - Consulté préalablement sur tous nouveaux traitements automatisés
    - Possibilité de saisir la CNIL
  - Liberté de l'employeur dans le choix éventuel d'un correspondant sous réserve que:
    - Le correspondant ne soit pas le responsable des traitements automatisés ou son représentant
    - Absence de conflits d'intérêts entre sa mission et ses activités exercées parallèlement
  - Information préalable de cette désignation aux représentants du personnel, puis notification à la CNIL
  - Cette désignation prend effet dans le mois qui suit la réception de la notification par la CNIL
  - Cessation fonctions:
    - Manquements aux devoirs de sa fonction
    - Démission, décharger de ces fonctions pour un motif autre que le manquement aux devoirs de sa fonction





Partenaire Média



1.1.8 L'obligation de déclaration

- Sanctions du défaut de déclaration à la CNIL : article 226-16 du code pénal
  - 5 ans d'emprisonnement
  - 300 000 euros d'amende pouvant aller jusqu'à 1 500 000 euros pour les personnes morales
  - Insertion du jugement dans un ou plusieurs journaux et son affichage, aux frais du condamné

- L'absence de déclaration à la CNIL interdit à l'employeur de mettre en œuvre son projet

- Le refus du salarié de se soumettre à un traitement non déclaré à la CNIL ne constitue pas une faute pouvant lui être imputé et justifiant son licenciement (Cass. Soc., 6 avril 2004, n°01-45.227)





1.2 Droits des salariés lors de l'utilisation des NTIC au sein de l'entreprise

- 1.2.1 Le droit d'information
- 1.2.2 Le droit d'accès
- 1.2.3 Le droit de rectification
- 1.2.4 Le droit d'opposition





1.2.1 Le droit d'information

– Article 32 de la loi du 6 janvier 1978 modifiée prévoit que toutes les personnes auprès desquelles sont recueillies des données à caractère personnel les concernant sont informées directement par le responsable du traitement des données:

- **De l'identité du responsable du traitement**, et le cas échéant, de celle de son représentant
- **De la finalité** poursuivie par le traitement auquel les données sont destinées
- **Du caractère obligatoire ou facultatif** des réponses
- **Des conséquences** éventuelles, à leur égard, d'un défaut de réponse
- **Des destinataires** ou catégories de destinataires des données
- Le cas échéant, **du transfert des données** à caractère professionnel envisagé à destination d'un Etat non membre de la Communauté européenne
- **De l'existence d'un droit d'accès, d'opposition et de rectification, ainsi que les coordonnées du service compétent** auprès duquel elles peuvent exercer leur droit





Partenaire Média



1.2.2 Le droit d'accès

- Définition :Toute personne justifiant de son identité à le droit d'interroger le responsable d'un fichier ou d'un traitement aux fins de savoir s'il détient des informations sur elle et en obtenir communication (article 39 de la loi de 1978 modifiée)

- Bénéficiaires : Toute personne physique justifiant de son identité

- Contenu :
  - La confirmation que les des données à caractère personnel la concernant font ou ne font pas l'objet d'un traitement
  - Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées
  - Le cas échéant, des informations relatives aux transferts des données envisagées à destination d'un Etat non membre de la Communauté européenne
  - La communication, sous forme accessible, des données à caractère personnel qui la concernent ainsi que toute information disponible quant à l'origine de celles-ci
  - Les informations permettant de connaître ou contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé





Partenaire Média



1.2.2 Le droit d'accès

- Demande effectuée au moyen d'une requête écrite adressé au responsable du traitement à laquelle est joint leur justificatif d'identité

- Réponse dans un délai de 2 mois. Le silence gardé pendant plus de 2 mois vaut décision de refus. Le refus doit être motivé et précisé les délais et voies de recours

- Limites au droit d'accès :
  - Demandes manifestement excessives : nombre, caractère systématique ou répétitif
  - Si contestation, la charge preuve du caractère manifestement excessif incombe au responsable du traitement des données





1.2.3 Le droit de rectification

- Article 6 et 40 de la loi du 6 janvier 1978
- Si la personne fichée constate que les informations sont:
  - Inexactes
  - Incomplètes
  - Équivoques
  - Périmées
  - Collecte, utilisation, communication ou conservation d'informations interdites

  Elle peut exiger, sans délai, leur modification par le responsable du traitement
- Si contestation, la charge de la preuve pèse sur le responsable du traitement
- Forme de la demande et délai de réponse de l'employeur: cf. droit d'accès
- Sanctions de l'inexécution des obligations de l'employeur: article R 625-12 du code pénal, contravention de 5ème classe





Partenaire Média



1.2.4 Le droit d'opposition

- Article 38 de la loi du 6 janvier 1978, modifié et renforcé par la loi n°2004-801 du 6 août 2004
- Toute personne a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement
- Ce droit s'exprime:
  - Par un refus de répondre lors d'une collecte non obligatoire de données
  - Par le refus de donner l'accord écrit obligatoire pour le traitement de données sensibles telles que les opinions politiques ou convictions religieuses
- Le salarié doit être mis en demeure d'exprimer son choix avant la validation définitive de ses réponses
- Si collecte orale des informations, le salarié est mis en mesure d'exercer son droit d'opposition avant la fin de la collecte des données le concernant





Partenaire Média



2. Les relations individuelles et les NTIC

- 2.1 La gestion du personnel et les NTIC
- 2.2 Le contrôle de l'activité des salariés et les NTIC
- 2.3 L'utilisation à des fins personnelles par les salariés des NTIC
- 2.4 Réseaux sociaux et droit du travail





2.1 La gestion du personnel et les NTIC

- 2.1.1 Le recrutement
- 2.1.2 La paie
- 2.1.3 L'archivage électronique





2.1.1 Le recrutement

- Principe de proportionnalité : article L 1121-1 du code du travail : Les informations demandées au candidat à un emploi ne peuvent avoir d'autre but que:
  - Apprécier la capacité du candidat à occuper l'emploi proposé
  - Apprécier les aptitudes professionnelles du candidat
- Article L 1221-6 du code du travail :
  - Informations demandées doivent présenter un lien direct et nécessaire avec l'emploi proposé
  - Candidat doit répondre de bonne foi
- Tout questionnaire d'embauche ou autres supports qui collectent des informations à caractère personnel doivent, préalablement à leur mise en œuvre, être déclarés à la CNIL
  - Déclaration normale à la CNIL
  - Dispense de déclaration à la CNIL, si désignation d'un correspondant à la protection des données à caractère personnel





Partenaire Média



2.1.1 Le recrutement

- Délibération de la CNIL, n°2002-17 du 21 mars 2002, précise les informations pouvant être demandées ou non à un candidat lors de son recrutement:
  - Interdiction de collecter des informations relevant de la vie privée du candidat
  - Interdiction de collecter des informations par des moyens frauduleux, déloyaux ou illicites
  - Interdiction de collecter et conserver, sauf accord exprès du candidat, des données nominatives qui directement ou indirectement, font apparaître les origines raciales, opinions politiques, philosophiques ou religieuses, appartenance syndicale, ou encore des informations relatives à la santé ou à la vie sexuelle du candidat
  - Interdiction d'établir des profils automatiques





Partenaire Média



2.1.1 Le recrutement

- **Article L 1221-9 du code du travail** : tout candidat à un emploi devra être expressément informé, préalablement à leur mise en œuvre, des méthodes et techniques d'aide au recrutement et d'évaluation utilisées à leur égard

- **Article L 2323-32 du code du travail** : information préalable du comité d'entreprise sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi





2.1.1 Le recrutement

– En définitive, la CNIL, dans sa délibération n°02-017 du 21 mars 2002, reprend donc les principes issus de la loi du 6 janvier 1978 :
  - Le traitement doit faire l'objet d'une déclaration ordinaire
  - Le principe de finalité doit être respecté
  - Les candidats doivent être informés de tout traitement de leur information
  - L'accord exprès des candidats en cas d'enregistrement de données dites sensibles
  - L'utilisation d'annonces ne correspondant pas à un poste à pourvoir est illicite
  - La détermination de profils par méthode automatisée est interdite
  - Les résultats obtenus doivent restés confidentiels





Partenaire Média



2.1.2 La paie

– Délibération de la CNIL, n°2004-097 du 9 décembre 2004, dispense l'employeur de déclaration pour:

- Les traitements de gestion de la paie (calcul et paiement du salaire, frais professionnels, etc.)
- La gestion des déclarations sociales et fiscales obligatoires : DADS, emploi des travailleurs handicapés
- Les registres obligatoires : registre unique du personnel

– Toutefois, maintien de l'ensemble des droits des salariés (opposition, accès, rectification, etc.) et des obligations de l'employeur (finalité des fichiers, information des salariés, conservation, etc.)





2.1.3 L'archivage électronique

– Les obligations légales en matière de gestion fiscale, comptable ou sociale imposent aux entreprises de conserver sur de longues périodes des documents contenant des données à caractère personnel

– L'archivage électronique doit respecter les principes issus de la loi du 6 janvier 1978

ORDRE DES EXPERTS-COMPTABLES Région Paris Ile-de-France



Partenaire Média



2.1.3 L'archivage électronique

- Respect du principe du droit à l'oubli : les archives courantes et intermédiaires ne doivent pas être conservées dans l'entreprise durant des durées excessives eu égard à leur finalité

- Les responsables de traitements doivent mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données archivées contre une diffusion ou un accès non autorisés, ou encore contre toute autre forme de traitement illicite

- L'accès aux archives intermédiaires doit être limité à un service déterminé et il doit être procédé à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et habilitation)



Partenaire Média



2.2 Le contrôle de l'activité des salariés et les NTIC

- 2.2.1 Les badges électroniques et cartes à puces magnétiques
- 2.2.2 La biométrie
- 2.2.3 Le comptage des communications téléphoniques
- 2.2.4 La vidéosurveillance
- 2.2.5 Les dispositifs de géolocalisation GSM/GPS





2.2.1 Les badges électroniques et cartes à puces magnétiques

– Ce système a pour finalités:
  - Le contrôle de l'accès à l'entrée et dans certains locaux de travail
  - La gestion des horaires variables et des temps de présence
  - La gestion de l'accès au restaurant d'entreprise et la mise en place d'un système de paiement
  - Le contrôle d'accès des visiteurs

– Chaque passage du badge dans un lecteur permet l'enregistrement de données relatives à son détenteur

– Risque d'utilisation détournée des données et traçage des déplacements des salariés





Partenaire Média



2.2.1 Les badges électroniques et cartes à puces magnétiques

- Obligation de déclaration préalable à la mise en œuvre du dispositif à la CNIL, sauf désignation d'un correspondant informatiques et libertés. A défaut, le refus d'un salarié d'utiliser son badge ne constitue pas un motif légitime de licenciement (Cass. Soc., 6 avril 2004, n°01-45.227)

- Norme n°42 du 8 janvier 2002 : déclaration simplifiée suffisante pour les contrôle d'accès à l'entreprise

- L'employeur doit veiller à ce que ces dispositifs n'entravent pas la liberté de circulation des délégués syndicaux et représentants du personnel au sein de l'entreprise

- Interdiction de suivre les déplacements internes des salariés dans l'entreprise, sauf zones à risque. Dans ce cas de figure, information des salariés et justification de ces mesures





2.2.1 Les badges électroniques et cartes à puces magnétiques

– Informations pouvant être collectées et traitées:

- Identité (nom, prénom, numéro de matricule interne, etc.)
- Vie professionnelle (service, JRTT, congés, autorisations d'absences, etc.)
- Badges (numéro et date de validité)
- Heures d'entrée et de sortie, numéro de porte utilisée)
- Si accès à un parking : numéro de place et numéro d'immatriculation, etc.

– Durée de conservation:

- Éléments d'identification des salariés : 5 ans après le départ du salarié
- Éléments relatifs aux déplacements : 3 mois au plus
- Informations relatives au contrôle du temps de travail : 5 ans
- Éléments relatifs aux motifs d'absence : 5 ans au plus, sauf dispositions légales contraires
- Paiement par retenue sur salarie : 5 ans





Partenaire Média



2.2.2 La biométrie

- Les dispositifs biométriques permettent **l'identification d'une personne par ses caractéristiques physiques, biologiques ou comportementales** : empreintes digitales, iris de l'œil, contour de la main, ADN, signature, démarche, etc.

- **Autorisation préalable** de la CNIL requise avant toute mise en œuvre de tels dispositifs

- Sauf motif sécuritaire, interdiction de constituer une base de données d'empreintes digitales

- Arrêt du TGI de Paris, 19 avril 2005, 1ère ch., section sociale, n°05/00382
  - Interdit la mise en place d'un système de pointage par empreintes digitales aux fins de contrôler l'activité des salariés
  - Un tel dispositif porte atteinte aux libertés individuelles et n'est justifié par aucun motif de sécurité ou de protection de l'activité exercée au sein des locaux de travail
  - Non respect du principe de proportionnalité





Partenaire Média



2.2.2 La biométrie

- 2.2.2.1 Le contour de la main
- 2.2.2.2 L'empreinte digitale





Partenaire Média



2.2.2.1 Le contour de la main

– Ce dispositif vise les traitements qui ont pour objet:
  - Le contrôle des accès aux locaux de l'entreprise
  - La gestion des horaires et des temps de présence
  - Le contrôle de l'accès au restaurant d'entreprise et la gestion de la restauration
  - Le contrôle d'accès des visiteurs

– Seul le gabarit du contour de la main est enregistrée et auquel est associé un numéro d'identification de la personne. Interdiction de conserver la photographie de la main

– Destinataires de ces informations:
  - Service du personnel
  - Service paie
  - Service gérant la sécurité des locaux
  - Service gérant la restauration d'entreprise





Partenaire Média



2.2.2.2 L'empreinte digitale

– Finalité du dispositif reposant sur la reconnaissance de l'empreinte digitale :
  - contrôle des accès à l'entrée et dans les locaux de travail, à l'exclusion du contrôle des heures de travail

– Stockage des données réalisées sur un support individuel dont le salarié a un contrôle exclusif

– Seul le gabarit de l'empreinte digitale est enregistrée

– Autorisation de la CNIL donnée au cas par cas





2.2.2.2. L'empreinte digitale

- **Délibération CNIL, n°2010-072 du 18 mars 2010**
  - La CNIL suspend durant 3 mois un dispositif de biométrie illégal, système de contrôle d'accès reposant sur la reconnaissance d'empreintes digitales, dans l'attente de la mise en conformité de l'entreprise:
    - Société n'avait pas tenu compte du refus d'autorisation de mise en œuvre du dispositif par la CNIL
    - Les salariés n'avaient pas été informés
    - L'entreprise conservait les données sans limitation de durée dans le temps





2.2.3 Le comptage des communications téléphoniques

- Permet l'enregistrement des numéros appelés pour chaque poste téléphonique ainsi que l'ensemble des éléments de communication (date, heure, durée, coût)

- Permet d'identifier les interlocuteurs

- Permet à l'employeur de maîtriser ses dépenses liées à l'utilisation des services de téléphonie

- Interdiction d'écouter ou d'enregistrer les conversations téléphoniques des salariés, ni même localiser un salarié à partir de son téléphone portable, sauf lorsque le travail consiste à téléphoner (ventes par correspondance, standardistes, etc.) Recommandation CNIL n°84-31 du 18 septembre 1984

- Connaître exactement le temps passé par chaque salarié à l'exécution de son travail





2.2.3 Le comptage des communications téléphoniques

- Bénéficie de la déclaration simplifiée à la CNIL (délibération du 3 février 2005, n°2005-019) pour les traitements des données relatives à l'utilisation du téléphone portable, dans le cadre professionnel

- Si les relevés téléphoniques font état des numéros de téléphone appelés, les 4 derniers chiffres doivent être occultés

- Les IRP doivent disposer de lignes téléphonique excluant toute possibilité d'interception ou d'indentification des correspondants (Délibération CNIL n°94-113 du 20 décembre 1994 et Cass. Soc., 6 avril 2004, n°02-40.498)

- L'ensemble de ces données sont conservées pendant un an, à compter de la date d'exigibilité des sommes dues au titre des communications téléphoniques





2.2.3 Le comptage des communications téléphoniques

- Par l'utilisation de la facturation détaillée
  - La simple vérification des relevés de la durée, du coût et des numéros des appels téléphoniques passés à partir de chaque poste, édités au moyen de l'autocommutateur téléphonique de l'entreprise, ne constitue pas un procédé de surveillance illicite pour n'avoir pas été préalablement porté à la connaissance des salariés (Cass. Soc., 29 janvier 2008, n°06-45.279)
  - La vérification par l'entreprise des relevés de ses communications téléphoniques fournies par France Télécom ne constitue pas un procédé de surveillance illicite des salariés pour ne pas avoir été porté à leur connaissance (Cass. Soc., 15 mai 2001, n°99-42.937)

- L'utilisation par un salarié du téléphone de l'entreprise à des fins personnelles n'est pas en soi fautive, sauf utilisation abusive (Cass. Soc., 29 janvier 2008, n°06-45.279)

- L'abus est caractérisé par:
  - Utilisation à répétition pendant de nombreuses heures de travail (CA Versailles 28 novembre 1995, n°94-22495)
  - Appels de longues distances (Cass. Soc., 18 juin 2003, n°01-43.122)





Partenaire Média



2.2.4 La vidéosurveillance

- 2.2.4.1 La vidéosurveillance dans les locaux de travail
- 2.2.4.2 La vidéosurveillance dans les autres locaux de l'entreprise





2.2.4.1 La vidéosurveillance dans les locaux de travail

– A titre de rappel:
  - Consultation préalable des IRP
  - Information individuelles des salariés concernés
  - Déclaration normale et préalable à la CNIL, sauf désignation d'un correspondant Informatiques et Libertés

– A défaut, la sanction est l'illicéité des moyens de preuve obtenus par l'employeur

– Délibération de la CNIL n°2010-112 du 22 avril 2010
  - Interruption d'urgence d'un dispositif de vidéosurveillance mise en œuvre par une société de transport routier pour lutter contre les dégradations matérielles et protéger les salariés
  - CNIL a constaté que ce dispositif plaçait les salariés sous surveillance constante, générale et permanente non justifiée





Partenaire Média



2.2.4.2 La vidéosurveillance dans les autres locaux de l'entreprise

– Quid du licenciement de salariés fondé des enregistrements vidéo recueillis, à leur insu, dans des locaux non affectés au travail des salariés: Cass. Soc., 19 avril 2005, n°02-46.295

- Le système de vidéosurveillance n'a pas vocation à contrôler l'activité des salariés
- Aucune consultation des IRP, ni même d'information des salariés sur ce système ne s'impose
- Moyen de preuve recueilli licite
  - **Cass. Soc., 19 janvier 2010, n°08-45.092**: l'employeur est libre de mettre en place un dispositif de surveillance dans des locaux où les salariés ne travaillent pas.
    - » Salarié surpris par un membre du service de gardiennage des locaux mis en place pour assurer leur protection contre les vols et dégradations, alors qu'il se trouvait sur le toit d'un bâtiment dont l'accès était interdit au personnel pour des raisons de sécurité: constatations de l'agent de sécurité peuvent être invoquées au soutien d'une mesure disciplinaire





Partenaire Média



2.2.5 Les dispositifs de géolocalisation GSM/GPS

– Certains employeurs équipent leurs véhicules professionnels de dispositifs de géolocalisation

– Par ce dispositif, risque d'atteinte à la liberté d'aller et venir et à la vie privée des salariés

– Mise en place:
- Déclaration simplifiée à la CNIL
- Information préalable des salariés concernés (finalité du traitement, des données traitées, durée conservation, destinataires des données, leurs droits)
- Information préalable des IRP





Partenaire Média



2.2.5 Les dispositifs de géolocalisation GSM/GPS

– **Finalités du dispositif**:
  - Le respect d'une obligation légale ou réglementaire imposant la mise en œuvre d'un dispositif de géolocalisation en raison du type de transport ou de la nature des biens transportés
  - Le suivi et la facturation d'une prestation de transport de personnes ou de marchandises ou d'une prestation de services directement liée à l'utilisation du véhicule
  - La sûreté ou la sécurité du salarié ou des marchandises ou du véhicule dont il a la charge
  - Une meilleure allocation des moyens pour des prestations à accomplir en des lieux dispersés
  - Le suivi du temps de travail, lorsque ce suivi ne peut pas être effectuer par un autre moyen

– Article 226-21 du code pénal punit le détournement de finalité de 5 ans d'emprisonnement et 300 000 euros d'amende

– **Limites du dispositif:**
  - Il ne doit pas conduire à un contrôle permanent du salarié, surtout si l'intéressé peut utiliser son véhicule à des fins privées
  - Les représentants du personnel ne peuvent faire l'objet d'une telle opération dans l'exercice de leur mandat





Partenaire Média



2.2.5 Les dispositifs de géolocalisation GSM/GPS

- Les données collectées vont permettre:
  - L'identification du salarié
  - L'identification des déplacements effectués
  - Informations complémentaires telles vitesse, temps de conduite, etc.

- A noter, que le traitement de la vitesse maximale est impossible car les infractions éventuelles ne doivent pas être identifiées

- Durée des conservation des données:
  - Principe: limitée à 2 mois, sauf réglementation contraire
  - Portée à un an, quand le dispositif a pour objectif :
    - La réalisation d'un historique des déplacements à des fins d'optimisation des tournées
    - Constitue le seul moyen de preuve de la réalisation de la prestation par le salarié
  - Portée à 5 ans, dans le cadre du suivi du temps de travail





Partenaire Média



2.3 L'utilisation à des fins personnelles par les salariés des NTIC

- 2.3.1 L'existence de règles d'utilisation des NTIC
- 2.3.2 La messagerie professionnelle
- 2.3.3 L'accès à internet
- 2.3.4 Le contrôle des fichiers stockés sur le disque dur de l'ordinateur des salariés

ORDRE DES EXPERTS-COMPTABLES
Région Paris Ile-de-France





2.3.1 L'existence de règles d'utilisation des NTIC

- Deux grands principes en concurrence:
  - **Article L 1121-1 du code du travail** relatif au respect à la vie privée du salarié: « *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* »
  - **Prérogatives de l'employeur**: Le droit disciplinaire qui vise à interdire tout usage abusif des NTIC par le salarié au temps et lieu de travail. L'abus se matérialise de deux façons:
    - L'abus au vu du contenu des messages ou sites visités
    - L'abus au vu de la fréquence et la durée d'utilisation des NTIC sur les lieux du travail

- Le contrôle de l'employeur doit donc être:
  - Justifié par l'intérêt de l'entreprise et respecter le principe de proportionnalité au but recherché
    - Bon fonctionnement des réseaux informatiques, la mise en jeu de la responsabilité de l'employeur, les coûts financiers pour l'entreprise
  - Le procédé de contrôle doit être fiable et transparent : information/consultation des représentants du personnel et information individuelle des salariés
  - Respecter la vie privée du salarié





Partenaire Média



2.3.1 L'existence de règles d'utilisation des NTIC

2.3.1.1 Les chartes d'éthiques ou déontologiques

2.3.1.2 Les dispositifs d'alertes professionnelles





2.3.1.1 Les chartes déontologiques ou d'éthiques

- Outils juridiques : la rédaction de chartes déontologiques
  - Annexées au règlement intérieur ou simplement portées à la connaissance des salariés
  - ❖ Attention, pour que la charte informatique ou déontologique soit opposable au salarié, il faut respecter les règles applicables en matière d'élaboration et de modification du règlement intérieur (en ce sens, Cass. Soc. 15 décembre 2010 n°09-42.691)
  - Permettent la clarification des règles d'utilisation et de fonctionnement des NTIC au sein de l'entreprise
  - Assurent l'information des salariés sur la mise en place d'éventuels moyens de surveillance
- Forme et contenu de la charte:
  - Soit un guide d'utilisation des différents outils informatiques mis à la disposition des salariés (procédures à suivre, mode d'emploi des diverses procédures à suivre). Elle fera l'objet d'une simple note de service, pouvant être modifiée sans formalisme ou procédure particulière
  - Soit un document générateur d'obligations pour les salariés (règles à respecter). Dans ce cas de figure, elle comporte nécessairement un volet disciplinaire et sera intégrée ou annexée au règlement intérieur. Par conséquent, lors de l'élaboration de la charte ou de sa modification ultérieure, l'employeur devra respecter la procédure de modification du règlement intérieur, article L 1321-4 du code du travail, à savoir:
    - Avis du CE ou à défaut des DP
    - Avis du CHSCT pour les mesures d'application de la réglementation en matière de sécurité de l'entreprise
    - Communication à l'inspecteur du travail
    - Publicité et affichage





Partenaire Média



2.3.1.1 Les chartes déontologiques ou d'éthiques

- Si la charte est génératrice d'obligations pour les salariés, elle contiendra:
  - Des règles d'utilisation des moyens informatiques de l'entreprise
  - Des règles de sécurité des moyens informatiques
  - Des procédures de contrôle de l'activité des salariés utilisateurs

- En tout état de cause, la mise en place d'une charte nécessite:
  - Rédaction de la charte en concertation avec les représentants du personnel. En pratique, rédaction unilatérale de l'employeur
  - Information/consultation du CE:
    - » Lors de l'introduction de nouvelles technologies dans l'entreprise, article L 2323-13 du code du travail
    - » Préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant le contrôle de l'activité des salariés article, L 2323-32 du code du travail
  - Information des salariés sur les modalités de contrôle
  - Déclaration préalable à la CNIL, si les règles édictées comportent la collecte d'informations nominatives concernant la manière dont chaque salarié utilise son ordinateur (nombre de messages reçus ou émis, sites consultés, etc.), à défaut:
    - Article 226-16 du code pénal : 5 ans d'emprisonnement et 300 000 euros d'amende
    - Interdiction pour l'employeur de se prévaloir des données ainsi recueillies : preuve illicite





Partenaire Média



2.3.1.2 Les dispositifs d'alertes professionnelles (ou whistleblowing)

- **Définition**: organisation des modalités selon lesquelles les salariés peuvent signaler à l'employeur des problèmes pouvant sérieusement affecter son activité ou engager sa responsabilité (hotline)

- **Mise en œuvre**:
  - Décision unilatérale de l'employeur ou par voie d'accord collectif
  - Si le dispositif comporte un traitement automatisé des données à caractère personnel : déclaration à la CNIL (article 25 loi du 6 janvier 1978 modifiée)
    - Soit par une déclaration d'engagement de conformité à la décision d'autorisation unique du 8 décembre 2005 1)
    - Soit après autorisation formelle de la CNIL
  - Consultation préalable du CE, article L 2323-32 du code du travail et éventuellement du CHSCT (TGI Nanterre 27 décembre 2006, n°06-2550)
  - Information individuelle et préalable des salariés utilisateurs et ceux mise en cause, article L 1222-4 du code du travail

2.3.1.2 Les dispositifs d'alertes professionnelles (ou whistleblowing)

- Usage de ce système constitue une faculté pour les salariés et l'anonymat doit pouvoir être conservé

- Destinataires des données :
  - A une organisation spécifique au sein de l'entreprise, astreinte à une obligation de confidentialité
  - Possibilité de recourir à un prestataire extérieur

- Durée conservation des données : Fonction de la nature des données
  - Donnée qui n'entre pas dans le champ d'application du dispositif : **archivage ou destruction immédiate**
  - Donnée qui fait l'objet d'une vérification sans suite disciplinaire ou judiciaire : **archivage ou destruction dans les 2 mois qui suivent la fin de la vérification**
  - Donnée qui fait l'objet d'une procédure disciplinaire ou judiciaire : **conservation jusqu'au terme de la procédure**





2.3.1.2 Les dispositifs d'alertes professionnelles (ou whistleblowing)

– Premières décisions jurisprudentielles sur le dispositif d'alerte professionnelle:

- **Dans un arrêt du 8 décembre 2009, n°08-17.191**, la Cour de cassation se prononce pour la première fois sur un dispositif d'alerte professionnelle.

  Elle juge ce dispositif illicite dans la mesure où il fait l'objet d'une simple déclaration de conformité auprès de la CNIL alors même que ce dispositif ne répondait pas à une obligation législative ou réglementaire de droit français visant à l'établissement de procédure de contrôle interne dans les domaines financiers, comptable, bancaire et de la lutte contre la corruption

  Une autorisation formelle de la CNIL était nécessaire

- **Dans une ordonnance de référé du TGI de CAEN du 5 novembre 2009**, **n°09-287**, le tribunal a décidé de suspendre sous astreinte l'utilisation du dispositif d'alerte professionnelle dans la mesure il permettait de dénoncer anonymement des faits allant au-delà d'actes de corruption ou de malversations mais autorisait la pratique de la délation contraire à l'article 8 de la loi du 6 janvier 1978 modifiée





2.3.2 La messagerie professionnelle

- **Articulation entre**:
  - Le droit disciplinaire de l'employeur qui peut sanctionner toute utilisation non professionnelle et excessive des moyens informatiques
  - Le droit des salariés, même pendant leur temps de travail, au respect de leur vie privée

- **Arrêt Nikon du 2 octobre 2001, n°99-42.942** :

  « le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée; que celle-ci implique en particulier le secret des correspondances; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci, même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur »





2.3.2 La messagerie professionnelle

– **Assimilation des messages électroniques à de la correspondance privée**
  - Décision du Conseil Constitutionnel du 10 juin 2004, n°2004-496 relative à la loi pour la confiance dans l'économie numérique
  - Jurisprudence constante : arrêt Nikon du 2 octobre 2001, n°99-42.942
  - Recommandation de la CNIL (fiche CNIL du Guide l'Employeur « *Le contrôle de l'usage de la messagerie électronique »)*





2.3.2 La messagerie professionnelle

- Si l'employeur entend contrôler l'usage de la messagerie électronique du salarié, il doit:
  - Préalablement informé le salarié du dispositif de contrôle mis en place, à défaut les moyens de preuve ainsi recueillies seront irrecevables car illicites
  - Justifier son contrôle par un intérêt légitime article L 1121-1 du code du travail (problème de sécurité, éviter un usage abusif ou préjudiciable à l'entreprise)
  - Procéder à une déclaration normale à la CNIL, sauf désignation d'un correspondant Informatiques et Libertés

- Le salarié est donc protégé par l'article 9 du code civil relatif au respect de la vie privée et par le principe du secret des correspondances émises par voie de télécommunications (loi du 10 juillet 1991, n°91-646)

- Sanction de l'atteinte au secret des correspondances : article 432-9 du code pénal « *Le fait (…) d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu des correspondances, est puni de 3 ans d'emprisonnement et de 45 000 euros d'amende* »



Partenaire Média



2.3.2 La messagerie professionnelle

– Principe : l'e-mail envoyé ou reçu depuis le poste de travail mis à la disposition par l'entreprise revêt un caractère professionnel et est donc susceptible d'être lu par l'employeur. L'employeur peut y accéder librement (Cass. Soc., 30 mai 2007, n°05-43.102)

- La réception de courriels pornographiques de collègues de travail ou de clients de l'entreprise n'est pas constitutive d'une faute grave (Cass. Soc. 14 avril 2010, n°08-43.258)
  – Cette réception ne démontre pas l'enregistrement pas le salarié de ces images sur son ordinateur professionnel

2.3.2 La messagerie professionnelle

- Exceptions :
  - Mention « personnel » dans l'objet du message ou dans le nom du répertoire d'archive par le salarié (CA de Besançon, 21 septembre 2004, n°03/1807)
    - Les messages électroniques échangés entre deux salariés de l'entreprise, au moyen de la messagerie interne, portant en objet: « PVI-PROJET IMPRO N-1 » ne permettait pas de présumer son caractère personnel: ouverture possible par employeur en l'absence des salariés concernés (CA POITIERS, ch. Soc., 2 février 2010, n°09/00137)
  - Termes et formulation du message (CA de Toulouse, 6 février 2003, n°02/02519 :référence aux vacances du salarié)
  - Accès protégé par un mot de passe
  - Messages échangés dans le cadre d'une adresse de messagerie personnelle du salarié, et non dans le, cadre de sa messagerie professionnelle (Cass. Soc., 9 avril 2009, n°08-12.503)





2.3.2 La messagerie professionnelle

- **Limites à l'usage personnel de la messagerie** : une utilisation abusive est fautive
  - Le contenu du message
    - L'envoi d'un courriel antisémite à partir de la messagerie de l'entreprise et permettant d'identifier l'entreprise constitue une faute grave **(Cass. Soc., 2 juin 2004, n°03-45.269)**
    - **CA de Limoges du 23 février 2009, n°08/01112** : le salarié critiquait la politique de gestion des sinistres menée par la société d'assurances et incitait l'ensemble des salariés à intenter une action en justice contre leur employeur et à signer une pétition contre lui (manquement à l'obligation de loyauté)
    - **CCAS de Nîmes du 11 juillet 2012 (Cass. Soc. N°11-22.225):** un salarié adresse à son employeur la lettre suivante: *« Je n'accepte pas ce type d'accusation hystérique émanant d'une personne inapte à émettre un jugement objectif sur mon travail ».*

    Licenciement pour motif réel et sérieux compte tenu du caractère non public des propos et des fonctions de responsabilité importantes qu'exerçait l'intéressé dans l'entreprise depuis des années.

    - **CCAS de Nîmes du 11 juillet 2012** (Cass. Soc. N°11-23.486): faute grave d'un salarié ayant adressé à son supérieur hiérarchique un courriel de reproches en ayant mis en copie les 13 membres de son équipe.





2.3.2 La messagerie professionnelle

- **L'utilisation excessive de la messagerie à des fins privées**

  - **CA de Limoges du 23 février 2009, n°08/01112** : utilisation habituelle voir systématique, à des fins privées, de la messagerie, faute d'avoir été autorisée ou tolérée par l'employeur, est fautive (dizaine de messages sur 11 jours avec une pointe de 7 messages sur une journée)

  - **CA de Rennes du 4 juillet 2000, n°99/4167** : utilisation pendant plusieurs mois de la messagerie de l'entreprise à des fins personnelles, avec des pointes à 18 messages par jour. La longueur et la répétition de ces messages ne pouvaient que distraire le salarié à l'exécution de son travail, d'autant que le salarié avait un poste à responsabilité et devait donc donner l'exemple



Partenaire Média



2.3.3 L'accès à internet

- Internet est un outil mis à la disposition du salarié par l'employeur pour un usage professionnel

- Le salarié ne dispose pas d'un droit à l'utilisation personnel de l'internet

- Toutefois, à l'instar de la messagerie professionnelle, il est difficile de refuser par principe toute utilisation personnelle d'internet sur les lieux de travail. L'employeur doit admettre un usage raisonnable personnel d'internet (Rapports CNIL du 23 mars 2001 et 5 février 2002)

- L'utilisation personnelle doit demeurer raisonnable. L'employeur est fondé à contrôler cette utilisation et poser des conditions d'usage de l'internet, conditions portées à la connaissance des salariés





2.3.3 L'accès à internet

- Principe: libre contrôle par l'employeur des connexions internet du salarié pendant son temps de travail

  - La jurisprudence considère que les connexions établies par un salarié sur des sites internet pendant son temps de travail grâce à l'outil informatique mis à sa disposition par l'employeur pour l'exécution de son travail <u>sont présumées avoir un caractère professionnel</u>, de sorte que l'employeur peut les rechercher aux fins de les identifier, hors la présence du salarié **(Cass. Soc., 9 juillet 2008, n°06-45.800)**

    - L'inscription d'un site sur la liste des « favoris » de l'ordinateur d'un salarié ne lui confère aucun caractère professionnel **(Cass. Soc., 9 février 2010, n°08-45.253): accès libre de l'employeur**





Partenaire Média



2.3.3 L'accès à internet

– Limites à l'usage personnel des connexions à internet:

- **Le contenu des sites visités**
  - Visites de sites érotiques ou pornographiques de nature à porter préjudice à la société dont le nom apparaissait à travers l'adresse mail utilisé par le salarié : faute grave (CA de Toulouse 4 septembre 2003, n°02/3683 et CA de DOUAI du 31 janvier 2007, n°06/530 et Cass. Crim., 19 mai 2004,n° 03-83.953 : salarié condamné pour abus de confiance)
  - Connexions régulières à des sites pédophiles dont la consultation est de nature à constituer l'infraction prévue à l'article 227-23 du code pénal, infraction dont l'employeur peut être tenu pour pénalement responsable : faute grave (CA de DOUAI du 28 février 2005, n°01/1258)
  - Création d'un site sadomasochiste en utilisant le matériel mis à la disposition par l'employeur :faute grave (CA de Grenoble, 10 novembre 2003, n°00/4741)
- **La fréquence et la durée d'utilisation** (affecte l'accomplissement du travail du salarié)
  - Utilisation à des fins privées des connexions internet de l'entreprise pour une durée totale d'environ 41 heures en un mois : faute grave (Cass. Soc., 18 mars 2009, n°07-44.247)
  - L'ampleur des connexions et leur fréquence sont de nature à affecter l'accomplissement par le salarié de son travail : faute grave (CA de DOUAI du 28 février 2005, n°01/1258). En l'espèce, correspondait à 8 heures par mois alors que le salarié passait environ la moitié de son temps dans des interventions extérieures





Partenaire Média



2.3.3 L'accès à internet

– Responsabilité civile de l'employeur (Art. 1384 al 5 du Code Civil)

- Liées aux connexions des salariés aux services à des fins non professionnelles (téléchargement musicaux contrevenant aux droits d'auteur, blog diffamatoire, incitation à la haine raciale, diffusion d'image à caractère pédophile, etc.)

- Responsabilité de plein droit: aucune faute personnelle de l'employeur n'est requise pour engager sa responsabilité du fait de ses salariés





2.3.4 Le contrôle des fichiers stockés sur le disque dur de l'ordinateur des salariés

– Principe : présomption du caractère professionnel des fichiers stockés sur le disque dur

Les fichiers créés par les salariés à l'aide de l'outil informatique mis à leur disposition par l'employeur pour les besoins de leur travail **sont présumés avoir un caractère professionnel** sauf si les salariés les identifient comme étant personnels, en sorte que l'employeur est en droit de les ouvrir hors la présence des salariés (Cass. Soc.18 octobre 2006, n°04-48.025 et 04-47.400).

- La mention du nom ou des initiales du prénom ne permettent pas de renverser cette présomption (Cass. Soc., 8 décembre 2009, n°08-44.840 et Cass. Soc., 21 octobre 2009, n°07-43.877)
- Les fichiers contenus dans un ordinateur dont le code d'accès n'est connu que des informaticiens et destiné à empêcher l'intrusion de personnes étrangères à celle-ci dans le réseau informatique, ne sont pas considérés comme personnels (Cass. Soc., 8 décembre 2009, n°08-44.840)
- La mention « essais divers, essais divers B, essais divers restauré » sur les fichiers ouverts par l'employeur ne permettent pas d'identifier leur caractère personnel (Cass. Soc., 15 décembre 2009, n°07-44.264)





Partenaire Média



2.3.4 Le contrôle des fichiers stockés sur le disque dur de l'ordinateur des salariés

- Le salarié qui stocke, sur son ordinateur professionnel, des fichiers à caractère pornographique, commet une faute grave (Cass. Soc., 16 mai 2007, n°05-43.455)

- La seule conservation par le salarié sur son poste informatique de 3 fichiers contenant des photos pornographiques sans caractère délictueux <u>ne constitue pas</u>, et en <u>l'absence de toute constatation d'un usage abusif</u> affectant son travail, un manquement aux obligations professionnelles permettant de justifier un licenciement (Cass. Soc., 8 décembre 2009, n°08-42.097)

- Un salarié qui avait volontairement procédé, avant d'être placé en arrêt maladie, à la mise en place d'un mot de passe personnalisé ayant pour conséquence de mettre obstacle à la consultation de fichiers professionnels par son employeur et ce malgré l'interdiction qui lui avait été faite à cet égard et qui avait refusé pendant son arrêt de travail de communiquer le mot de passe grâce auquel il était possible d'accéder aux données, commet une faute grave (Cass. Soc. 23 mai 2012 n°11-11.522)

2.3.4 Le contrôle des fichiers stockés sur le disque dur de l'ordinateur des salariés

– Cas des fichiers identifiés comme personnels par le salarié : conditions de licéité du contrôle de l'employeur (Cass. Soc., 17 mai 2005, n°03-40.017 et 17 juin 2009, n°08-40.274 et CA de RENNES, n°09/03817 du 11 mars 2010):

- Ouverture des fichiers **en présence du salarié** ou qu'il ait été **dûment appelé**, à défaut moyen de preuve illicite
  – Ouverture en présence du salarié, assisté d'un homme de loi, et du représentant de l'employeur: aucune violation des droits du salarié (CA BORDEAUX, n°08/01453 du 24 novembre 2009

- En l'absence du salarié, dans le cas d'un **risque ou évènement particulier**





2.3.4 Le contrôle des fichiers stockés sur le disque dur de l'ordinateur des salariés

– Quid de la notion de risque ou évènement particulier:

Selon la doctrine, il s'agirait d'un impératif immédiat de sécurité, l'urgence absolue à une telle ouverture est donc requise, ou de très graves délits pénaux tels des menaces terroristes, pédophilie, proxénétisme, etc. (Droit social, n°7/8-2005 « *L'ouverture par l'employeur des dossiers personnels du salarié* » Jean-Emmanuel REY)

- À la suite d'un incident de sécurité sur un site classé SEVESO, l'employeur peut confier, conformément à la charte informatique, une enquête spécifique à l'administrateur des systèmes soumis à une obligation de confidentialité sur les ordinateurs mis à disposition des salariés, il est possible qu'au travers d'une telle enquête de grande amplitude et en l'absence de référence aux courriers personnels, l'employeur ait eu accès à des messages personnels. Dans ce cas, les représentants du personnel peuvent demander à être associés à cette enquête **(Cass. Soc., 17 juin 2009, n°08-40.274)**

2.3.4 Le contrôle des fichiers stockés sur le disque dur de l'ordinateur des salariés

L'ouverture du disque dur s'effectue selon deux modalités distinctes:

– Requête déposée auprès du TGI aux fins d'intervention d'un huissier de justice
  - La jurisprudence considère que le respect de la vie privée du salarié ne constitue pas en lui-même un obstacle à l'application de l'article 145 du code de procédure civile (expertise in futurum), dès lors que le juge constate que les mesures qu'il ordonne procèdent d'un motif légitime et sont nécessaires à la protection des droits de la partie qui les a sollicitées (Cass. Soc., 23 mai 2007, n°05-17.818 et Cass. Soc., 10 juin 2008, n°06-19.229: salarié suspecté d'actes de concurrence déloyales dans les deux affaires)
  - L'huissier peut procéder:
    – À une sauvegarde du disque dur du salarié
    – Au constat d'existence et d'ouverture de certains fichiers
    – À la recherche de fichiers supprimés par le salarié

– Intervention des services de police ou de gendarmerie





Partenaire Média



2.4 Réseaux sociaux et droit du travail

- **Problématique:**
  - Les réseaux sociaux tels que Facebook, Myspace ou Twitter sont externes à l'entreprise et échappent à la relation du travail et au droit du travail
  - Contrairement à un blog ou à un site internet, l'accès est limité aux seules personnes acceptées par le détenteur du profil, c'est un réseau privé
  - L'internaute est « ficheur » en diffusant des informations sur lui-même et sur les autres et « fiché » en devenant un cible potentielle
  - Questions juridiques sur le droit à l'image, la diffusion d'informations confidentielles, le respect de la vie privée





2.4 Réseaux sociaux et droit du travail

- Principe
  - Respect de la vie privée du salarié
    - Article 9 du Code Civil
    - Article 8 CEDH
    - Article L 1121-1 du Code du Travail
  - Respect de la liberté d'expression dans et hors de l'entreprise
    - Interdiction de licencier sauf abus: dénigrement, injure, diffamation

- Interdiction de licencier pour un fait relevant de la vie personnelle du salarié

ORDRE DES EXPERTS-COMPTABLES
Région Paris Ile-de-France



Partenaire Média



2.4 Réseaux sociaux et droit du travail

- **Exceptions:**
  - Licenciement non disciplinaire en présence d'un trouble caractérisé pour l'entreprise: CRS
  - Licenciement disciplinaire:
    - Arrêts isolés: en raison des perturbations occasionnées dans le fonctionnement de l'entreprise
    - Faits commis en dehors du temps de travail qui se rattachent nécessairement à la vie professionnelle du salarié





2.4 Réseaux sociaux et droit du travail

- Un salarié peut-il être sanctionné pour avoir critiqué son employeur sur facebook ou sur tout autre réseau social?
  - Les propos tenus relèvent-ils du domaine privé ou public?
    - A priori, pas de difficulté s'agissant des messages échangés via Facebook
    - Quid des messages publiés sur « le mur » de la page facebook, uniquement accessibles aux amis?

  - Les propos tenus sont-ils injurieux ou excessifs?





2.4 Réseaux sociaux et droit du travail

– Le CPH de Boulogne Billancourt vient de rendre un arrêt de départage le 20 mai 2010 sur le sujet

- Faits: en décembre 2008, un soir, lors d'une conversation privée, 3 salariés d'une entreprise des Hauts-de-Seine évoquent leur activité professionnelle, égratignant au passage leur hiérarchie et le responsable RH. En référence à cette conversation, l'un d'eux écrit sur sa page personnelle facebook faire « partie d'un club des néfastes ». Les 2 autres répondent « Bienvenue au club ». Un 4ème salarié de l'entreprise et amis facebook décode le message et le transmet à la direction de l'entreprise.

- Les 3 salariés sont licenciés pour faute « dénigrement de l'entreprise » et « incitation à la rébellion »

- CPH saisi par 2 des 3 salariés

- Cette décision en attente pourrait faire jurisprudence





3. Les relations collectives et les NTIC

- 3.1 Le droit syndical face aux NTIC
- 3.2 Le comité d'entreprise et les NTIC





Partenaire Média



3.1 Le droit syndical face aux NTIC

- 3.1.1 Les conditions d'utilisation des NTIC par les syndicats : les tracts syndicaux
- 3.1.2 Le panneau d'affichage électronique
- 3.1.3 Les blogs





3.1.1 Les conditions d'utilisation des NTIC par les syndicats: les tracts syndicaux

- **La loi du 4 mai 2004, n°2004-391 relative à la formation tout au long de la vie professionnelle et au dialogue social** a complété les dispositions de l'article L 2142-6 du code du travail pour fixer les conditions d'utilisation par les organisations syndicales de l'intranet de l'entreprise ou de sa messagerie électronique:
  - Article L 2142-6 du code du travail : nécessité de conclure un accord d'entreprise avec l'employeur aux fins de permettre l'utilisation à des fins syndicales des nouvelles technologies et selon les modalités retenues par l'accord
  - Cet accord peut autoriser la mise à disposition des publications et tracts de nature syndicale, soit sur un site syndical mis en place sur l'intranet de l'entreprise, soit par diffusion sur la messagerie électronique des salariés
  - Cet accord doit définir les modalités de mise à disposition ou de ce mode de diffusion en précisant notamment:
    - Les conditions d'accès des organisations syndicales
    - Les règles techniques visant à préserver la liberté de choix des salariés d'accepter ou non un message électronique





Partenaire Média



3.1.1 Les conditions d'utilisation des NTIC par les syndicats: les tracts syndicaux

- **Respect du principe de finalité** : les adresses de messageries électroniques des salariés ne peuvent être utilisées par les organisation syndicales à des fins autres que la mise à disposition des publications et tracts de nature syndicale

- Cass. Soc. 19 mai 2010, n°09-40.279
  - L'accord d'entreprise autorisait la diffusion de tracts syndicaux par voie électronique dans la limite d'un certain quota et subordonnait cette diffusion, au-delà de ce quota, à l'autorisation de l'employeur, la cour d'appel a exactement retenu que la salariée avait commis une faute en utilisant la messagerie électronique de l'entreprise pour la distribution de tracts syndicaux au-delà du quota autorisé par l'accord collectif et décidé qu'il n'y avait pas lieu à annulation de la mise à pied disciplinaire de la salariée





3.1.1 Les conditions d'utilisation des NTIC par les syndicats : les tracts syndicaux

- Compatibilité de la diffusion de ces messages avec les exigences du bon fonctionnement du réseau informatique de l'entreprise et l'absence d'entrave à l'accomplissement du travail

- Le droit d'opposition des salariés : l'accord d'entreprise doit préciser les règles techniques visant à préserver la liberté de choix des salariés d'accepter ou non un message émanant des organisations syndicales. Ainsi, la CNIL recommande l'indication du caractère syndical du message en objet de façon à informer les intéressés de l'origine et de la nature du message

- La garantie de confidentialité des messages entre les salariés et les organisations syndicales

- Circulaire DRT n°9 du 22 septembre 2004 : les organisations syndicales non signataires bénéficient des droits reconnus aux organisations syndicales signataires, sous réserve de respecter strictement les termes de l'accord d'entreprise ainsi que les règles d'utilisation des outils mis à disposition





3.1.1 Les conditions d'utilisation des NTIC par les syndicats : les tracts syndicaux

– Quid en l'absence d'accord d'entreprise?

- Licéité d'un site syndical extérieur à l'entreprise sous réserve de respecter (TGI de Paris, 17 novembre 1978, n°97-64146):
  - Les règles de responsabilité générales posées par le code civil
  - La loi sur le presse de 1881
  - La loi sur la communication audiovisuelle de 1982
  - La loi sur les liberté de la communication de 1986
  - La loi sur la confiance dans l'économie numérique du 21 juin 2004

- Illicéité de la diffusion des publications ou tracts syndicaux par e-mail, sauf autorisation exprès de l'employeur (CA de PARIS du 3 mars 2004, n°2002/01008 et Cass. Soc. du 25 janvier 2005, n°02-30.946)

- La méconnaissance de ces dispositions constituent un trouble manifestement illicite dont l'employeur peut obtenir du juge des référés qu'il ordonne sous astreinte au syndicat de cesser d'utiliser ce mode de diffusion (CA de ROUEN du 18 mars 2003, n°01/3341 et Cass. Soc. du 25 janvier 2005, n°02.30-946)





Partenaire Média



3.1.2 Le panneau d'affichage électronique

- Article L 2142-3 du code du travail prévoit que « *L'affichage des communications syndicales s'effectue librement sur des panneaux réservés à cet usage et distincts de ceux qui sont affectés aux délégués du personne et du comité d'entreprise »*

- C'est donc par accord collectif que l'employeur fixe les règles matérielles d'utilisation des panneaux d'affichage ainsi que leurs conditions d'emplacement dans l'entreprise

- Rien n'interdit aux délégués syndicaux et à l'employeur de négocier un accord sur l'utilisation et les conditions d'emplacement de panneaux d'affichage virtuels, consultables sur l'intranet de l'entreprise

- Il s'agira d'une déclinaison du panneau sur support papier devant se conformer aux exigences de l'article L 2142-3 du code du travail:
  - Le panneau d'affichage virtuel devra respecter une certaine dimension
  - Le panneau informatique n'est qu'un espace de consultation, simple mise à disposition des salariés d'informations
  - Chaque communication syndicale devra être transmise à la Direction, simultanément à sa publication sur le site intranet de l'organisation syndicale





Partenaire Média



3.1.3 Les blogs

- Contrairement au site web classique, le blog repose sur un mode de publication relativement simple qui ne nécessite aucune connaissance technique. On trouve ainsi nombre de blog de salariés ou d'anciens salariés s'estimant lésés. Cette pratique des blogs permet ainsi à un salarié de rapporter un large public le conflit de nature personnelle qui l'a opposé avec son employeur

- Problème : le blog et le site internet sont externes à l'entreprise et échappe à la relation de travail et au droit du travail
  - L'article L 2142-4 du code du travail relatif à la diffusion des tracts syndicaux est inopérant puisque l'action syndicale intervient en dehors du périmètre de l'entreprise. Dans ce cas, sont applicables:
    - Les dispositions relatives à la loi sur la confiance dans l'économie numérique du 21 juin 2004, n°2004-575
    - Les dispositions relatives à la presse du 29 juillet 1881

      « Les propos contenus dans les tracts distribués au public (à l'extérieur) et qualifiés d'injurieux et diffamatoires par l'employeur ne peuvent être incriminés qu'au regard de la loi du 29 juillet 1881 » (Cass. Soc., 28 février 2007, n°05-15.228)
  - L'article L 2281-1 du code du travail relatif au droit d'expression direct et collectif est un droit spécifique qui n'est pas non plus applicable puisque c'est la liberté d'expression qui est en cause





Partenaire Média



3.1.3 Les blogs

– Quid de leur responsabilité?

S'agissant des anciens salariés, il convient de se placer sur le terrain de la liberté d'expression. Le blogueur pourrait engager sa responsabilité, non en plus en raison de son fait, mais de celui des internautes qui déposent des messages sur son blog sans cadre légal.

S'agissant des salariés d'une entreprise, ils sont soumis à une obligation de loyauté et de discrétion, y compris sur leur blog

- Principe : application de la liberté d'expression qui est une liberté publique prévue par les articles 10 et 11 de la DDHC de 1789
- La liberté d'expression ne se confond pas avec le droit d'expression dont le régime est encadré par le droit du travail





3.1.3 Les blogs

- **Limites à la liberté d'expression :**
  - Obligation de loyauté et de discrétion
  - Article L 2281-3 du code du travail précise que :
    « *Les opinions que les salariés, quelle que soit leur place dans la hiérarchie, émettent dans l'exercice de leur droit d'expression ne peuvent motiver une sanction ou un licenciement* », à condition de ne pas utiliser:
    - des propos injurieux, diffamatoires ou excessifs (Cass. Soc. 14 juin 2005, n°02-47.455),
    - de critiques portant atteinte à l'honneur, malveillantes ou excessives (Cass. Soc., 14 janvier 2003, n°00-43.879) ou susceptibles de perturber le bon fonctionnement de l'entreprise (Cass. Soc., 4 février 1997, n°96-40.678)
  - Sauf abus, le salarié jouit dans l'entreprise et en dehors de celle-ci , de sa liberté d'expression. Seules des restrictions justifiées par la nature de la tâche à accomplir et proportionnés au but recherché peuvent y être apportées (Cass. Soc., 22 juin 2004, n°02-42.446 et Cass. Soc., 21 février 2007, n°04-48.760)
  - Si la liberté d'expression dans l'entreprise et en dehors de celle-ci ne peut justifier un licenciement, c'est à la condition qu'elle ne dégénère pas en abus (Cass. Soc., 5 octobre 2004, n°02-44.487)





Partenaire Média



3.1.3 Les blogs

- Le salarié est tenu de procéder préalablement à une enquête sérieuse empreinte d'objectivité pour être à même de justifier ses propos par des éléments sérieux (TGI de Paris du 16 octobre 2006, n°06-8820)

- Si le salarié reproduit sur son site des informations nominatives concernant des personnes (nom, prénom, adresse, numéros de téléphone, etc.), sans autorisation, il contrevient aux dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (TGI de Paris du 16 octobre 2006, n°06-8820) : obligation de déclarer à la CNIL toute information à caractère personnel (et non de déclarer son blog)

- Si le salarié reproduit sur son blog une image extraite d'une publicité concernant la société à laquelle il est ou a été salarié, il contrevient aux dispositions de l'article L 122-4 du code de la propriété intellectuelle, dans la mesure où il s'agit d'une œuvre de l'esprit sur laquelle la société dispose de droit d'auteur et dont le reproduction, sans autorisation, est interdite (TGI de Paris du 16 octobre 2006, n°06-8820)





3.1.3 Les blogs

- Le TGI peut ordonner aux hébergeurs ou à défaut, au fournisseur d'accès toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne

  - TGI de Bobigny, n°04/13069 du 11 janvier 2005, TNS SECODIP / FEDERATION CGT DES SOCIETES D'ETUDES : ordonne la suppression de certaines pages d'un site syndical révélant des informations susceptibles de porter préjudice à l'entreprise



Partenaire Média



3.2 Le comité d'entreprise et les NTIC

- 3.2.1 Moyens d'information et de communication mis à la disposition du CE
- 3.2.2 Utilisation des moyens nouveaux de communication par le CE
- 3.2.3 Elections professionnelles par voie électronique





Partenaire Média



3.2.1 Moyens d'information et de communication mis à la disposition du CE

– Aucun texte ne régit les conditions d'utilisation de la messagerie électronique ou l'internet en ce qui concerne le CE, l'article L 2325-12 du code du travail se limitant aux tracts et communications syndicales

– Préférable de mettre en place un accord sur l'utilisation de ces nouveaux moyens technologiques (accord collectif, adjonction au règlement intérieur du CE, élaboration d'une charte informatique, etc.)

– L'article L 2325-12 dernier alinéa du code du travail dispose que « *Le chef d'entreprise doit mettre à la disposition du comité d'entreprise le matériel nécessaire à l'exercice de ses fonctions* »

– Sur ce point, une réponse ministérielle du 9 janvier 1989 précise que ce matériel doit être adapté aux besoins de comité et tenir compte de l'évolution technologique

3.2.1 Moyens d'information et de communication mis à la disposition du CE

- Matériel informatique
  - Article L 2325-12 dernier alinéa du code du travail : le législateur laisse le soin à chaque entreprise d'apprécier ce qu'il convient de considérer comme étant du matériel nécessaire à l'exercice des fonctions du CE
  - Si l'on observe qu'au sein de l'entreprise la majorité des agents administratifs dispose d'un ordinateur pour l'exercice de ses fonctions, alors le CE pourra légitimement prétendre au bénéfice d'un ordinateur

- Connexion informatique au sein de l'entreprise
  - Si en général, les salariés exerçant une activité administrative dans l'entreprise disposent d'une connexion internet et/ou intranet, l'employeur devra veiller à attribuer une connexion, dans les mêmes conditions, au CE
- Adresse de messagerie
  - Si l'employeur attribue une connexion sur le réseau intranet ou internet, il devra veiller à lui attribuer une adresse de messagerie du type: « comite-dentreprise@nom de l'entreprise.com »
  - L'entreprise peut allouer à chaque membre du CE élu ou désigné une adresse de messagerie spécifique pour l'exercice de son mandat
  - Confidentialité des échanges électroniques






Partenaire Média



3.2.1 Moyens d'information et de communication mis à la disposition du CE

– Contrepartie de cette mise à disposition : Contrôle et maintenance du matériel informatique

- Obligation pour le CE de faire régulièrement contrôler ce matériel et assurer la maintenance selon les normes fixées par le service informatique de l'entreprise
- Les membres sont astreints à une utilisation normale et doivent respecter les règles de sécurité les plus élémentaires (anti-virus)
- Les membres du CE ne doivent pas mettre en péril le système informatique de l'entreprise





Partenaire Média



3.2.2 Utilisation des moyens nouveaux de communication par le CE

– Communication avec l'employeur:
  - **Élaboration de l'ordre du jour** : messagerie interne peut être utilisé pour les échanges entre le secrétaire et le président qui doivent élaborer conjointement l'ordre du jour
  - **Transmission de documents** : utilisation de la messagerie et des fichiers joints pour permettre à la direction ou au secrétaire d'échanger des documents nécessaires à la préparation et à la bonne tenue des réunions du CE
  - **Convocation des membres**
  - **Circulation du projet de procès verbal**
  - **Affichage et diffusion du procès verbal** : mise à disposition du PV sur son site à la condition que la consultation soit réservée au personnel de l'entreprise sans accès possible aux personnes étrangères

– Communication interne entre les membres du comité:
  - Les membres du CE peuvent communiquer entre eux au moyen de la messagerie intranet lorsque l'employeur alloue à chaque membre une adresse de messagerie spécifique
  - Utilisation dans le respect de la confidentialité des échanges





Partenaire Média



3.2.2 Utilisation des moyens nouveaux de communication par le CE

- Communication avec les salariés de l'entreprise:
  - L'utilisation doit respecter les principes suivants:
    - Bon fonctionnement et règles de sécurité du réseau
    - Liberté du contenu des messages
    - Liberté pour les salariés de recevoir et lire ses messages
  - Échanges individuels
    - Doit s'effectuer en dehors des heures de travail du salarié ou pendant le temps de pause
  - Communication à l'ensemble du personnel
    - La loi ne permet pas au CE d'imposer sous quelque forme que ce soit, sur le lieu de travail la transmission de communications à l'ensemble du personnel de l'entreprise
  - Panneaux électroniques
    - Employeur peut proposer au CE la mise en place d'un panneau électronique venant compléter le panneau d'affichage classique
    - Mise en place d'un site intranet librement consultable par les salariés en dehors de leur temps de travail





Partenaire Média



3.2.2 Utilisation des moyens nouveaux de communication par le CE

- Gestion des activités sociales et culturelles
  - Dispensée de toute formalité déclarative préalable à la CNIL lorsque le système mis en place est conforme à la délibération adoptée le 17 octobre 2006, n°2006-230, c'est-à-dire, accorde aux salariés des droits d'opposition, d'accès et de rectification des données





Partenaire Média



3.2.3 Élections professionnelles par voie électronique

– Le décret n°2007-602 du 25 avril 2007 vient préciser les règles encadrant le vote électronique pour les élections professionnelles : articles R 2314-8 à R2314-21 du code du travail

- Conclusion d'un accord préélectoral
  - – Conclusion d'un accord d'entreprise ou de groupe comportant un cahier des charges respectant les prescriptions minimales du droit électoral
  - – Le protocole d'accord préélectoral doit mentionner la conclusion de l'accord d'entreprise ou de groupe autorisant le recours au vote électronique, et le cas échéant, le nom du prestataire choisi pour le mettre en place
  - – Comporte en annexe la description détaillée du fonctionnement du système retenu et déroulement des opérations électorales

- Avant le scrutin, l'employeur doit informer et former
  - – Chaque salarié dispose d'une notice d'information détaillée sur le déroulement des opérations électorales
  - – Formation des membres des IRP concernées





Partenaire Média



3.2.3 Élections professionnelles par voie électronique

- **Choix du prestataire de service par l'employeur**
  - Le système doit assurer la confidentialité des données transmises, sécurité des moyens d'authentification, d'émargement et de dépouillement des votes
- **Pendant le scrutin**
  - Mise en place d'une cellule d'assistance technique par l'employeur, chargée de veiller au bon fonctionnement et à la surveillance du vote électronique
  - La cellule d'assistance technique, en présence des représentants de liste:
    - » Procède, avant le scrutin, à un test du système du vote électronique et du système de dépouillement
    - » Vérifie que l'urne électronique est vide, scellée et chiffrée par des clés délivrés à cet effet
    - » Contrôle à l'issue des opération de vote et avant le dépouillement, le scellement de ce système
  - Vote électronique se déroule pendant un temps limité, pour chaque tour de scrutin
- **Le vote électronique n'interdit pas le vote à bulletin secret sous enveloppe, si l'accord n'exclut pas cette modalité**
- **Conservation des fichiers sous scellés jusqu'à:**
  - L'expiration du délai de recours
  - Si action contentieuse intentée, jusqu'à la décision juridictionnelle définitive

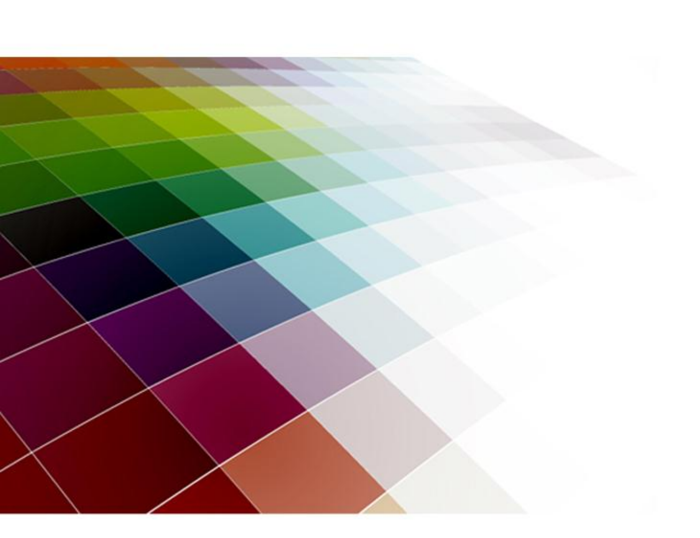
… Après destruction des fichiers supports





Partenaire Média







Ordre des experts-comptables région Paris Ile-de-France

50, rue de Londres • 75008 PARIS

www.oec-paris.fr

Contact :
Sylva Bilez • Tél. : 01 55 04 31 27 • sbilez@oec-paris.fr





Partenaire Média

